US005848161A

United States Patent [19]

Luneau et al.

[11] Patent Number: 5,848,161

[45] Date of Patent: Dec. 8, 1998

[54] METHOD FOR PROVIDING SECURED COMMERICAL TRANSACTIONS VIA A NETWORKED COMMUNICATIONS SYSTEM

[76] Inventors: **Greg Luneau**, Unit 603-110 Adamar Road, Winnipeg, MB, Canada, R3T 3M3; **Jason Remillard**, #8-100 Wickham Road, Winnipeg, MB, Canada, R2J 2L4; **Thomas King**, 637 W. Sunset Dr., Villa Park, Ill. 60181-1416

[21] Appl. No.: **648,876**

[22] Filed: **May 16, 1996**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/49**; 380/24

[58] **Field of Search** 380/23, 24, 25, 380/28, 30, 29, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,557,518	9/1996	Rosen	380/24
5,671,279	9/1997	Elgamal	380/24
5,673,316	9/1997	Auerbach et al.	380/25

OTHER PUBLICATIONS

"Doing Business on The Net", May 14, 1996 San Diego Tribune, Computer Link Section.

Tsudik, "Datagram Authentication in Internet Gateways:" III Journal on Selected Areas of Communication v7 n4, May 1989.

"Secure Electronic Tranaction Specification", Feb. 23, 1996 Mastercard/Visa.

"PGP Means Business", Jan. 1, 1996, Viacrypt.

"CyberCash Investors See Dollar Signs", Feb. 16, 1996 USA Today, p. 3B.

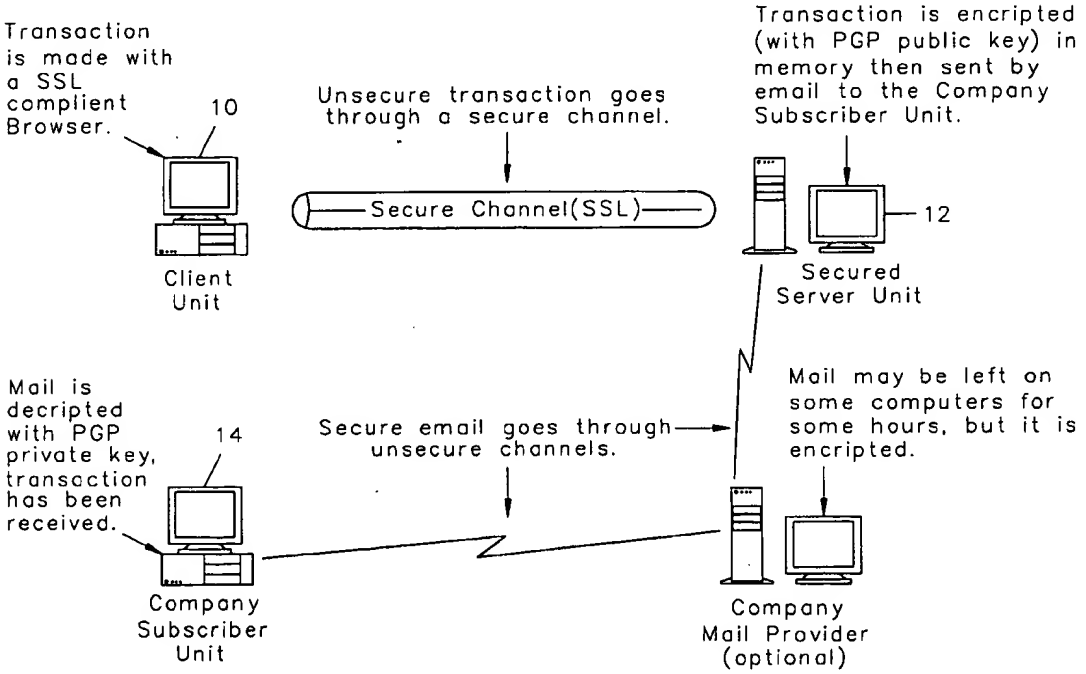
Primary Examiner—David Cain

Attorney, Agent, or Firm—Patnaude Videbeck & Marsh

[57] **ABSTRACT**

In a networked communications system comprising a client unit, a secured host server, and a company subscriber unit, a method for providing secured commercial transactions via the networked communications system. The method includes the steps of providing a secured transmission path via the networked communications system between the client unit and the secured host server, presenting the client unit with an order form in which commercial information is to be entered via the secured transmission path, receiving the commercial information transmitted via the secured transmission path by the client unit at the secured host server, maintaining the commercial information solely in the dynamic memory of the secured host server, encrypting the commercial information in response to the step of receiving the commercial information, erasing the dynamic memory of the secured host server in response to the step of encrypting the commercial information, and forwarding the encrypted commercial information via the communications network from the secured host server to the company subscriber unit.

8 Claims, 1 Drawing Sheet



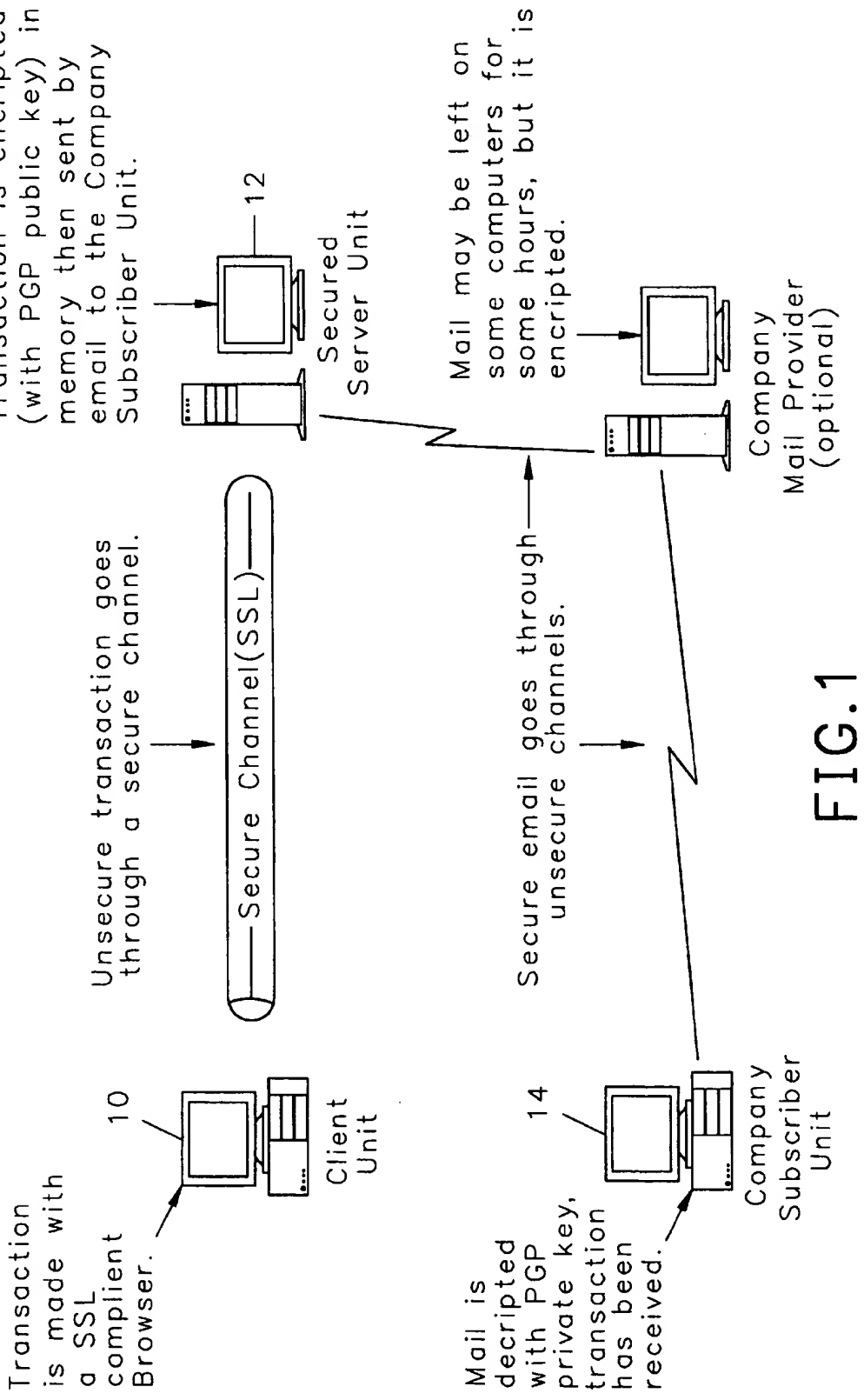

Transaction is encripted (with PGP public key) in memory then sent by email to the Company Subscriber Unit.
12
Secured Server Unit
Mail may be left on some computers for some hours, but it is encripted.
Company Mail Provider (optional)
Unsecure transaction goes through a secure channel.
Secure Channel(SSL)
Secure email goes through unsecure channels.
Transaction is made with a SSL compliant Browser.
10
Client Unit
14
Company Subscriber Unit
Mail is decripted with PGP private key, transaction has been received.

FIG. 1

METHOD FOR PROVIDING SECURED COMMERICAL TRANSACTIONS VIA A NETWORKED COMMUNICATIONS SYSTEM

BACKGROUND OF THE INVENTION

This invention relates generally to networked communications systems and, more particularly, relates to a method for providing secured commercial transactions between a client unit and a company subscriber unit via a global network known as the "Internet".

Currently, there are three major Secure Electronic Transaction (SET) payment schemes which have been developed and implemented. Each of these schemes utilizes cryptography for the purpose of providing confidentiality of information, ensuring payment integrity, and authenticating both merchants and cardholders. These security criteria are provided in hopes of enabling greater bank card acceptance combined with a level of security that will encourage consumers and businesses to make wide use of bank card products in this emerging market. In particular, the three SET payment schemes can be classified as follows: payment schemes using encrypted data; payment schemes using third parties; and payments using digital cash. A brief explanation and implementation examples of each payment scheme follow.

Payments Using Encrypted Data

With this payment scheme, credit card details are encrypted before they are transmitted to the merchant. The leading protocols used to establish the three security criteria above-described are secured sockets layer "SSL" and Secure HTTP "S-HTTP" which have been designed by RSA Data Security Inc. for Netscape and Enterprise Integration Technologies for NCSA Mosaic respectively. These two protocols are parallel security protocols. (Recently, a decision was announced by Netscape that both of these protocols would become integrated since they are deemed complementary.) Specifically, SSL provides the encryption necessary to route data to the merchants server while the S-HTTP protocol provides for security at the server itself.

In particular, these protocols both use public-key encryption to provide secure links. Public-key encryption uses a pair of keys whereby messages encoded by one key can only be decoded by the other key of that pair, and vice versa. Every working party has a unique set of keys where one key is kept secret and the other key is made public. This differs from secret-key encryption which utilizes one and the same key for encoding and decoding.

By way of example, public-key encryption generally works as follows: for authentication, a party encrypts with a secret key; verification is provided by decoding using the parties public key; and for private communication, the sending party encrypts using the other party's public key.

For examples of this payment scheme implemented, see The Netscape Galleria.

While this scheme is advantageous since the application is transparent to the end-user and it provides enhanced security, it nevertheless suffers the disadvantages of relying on codes that can be theoretically broken and is costly to implement in terms of added equipment and overhead. Furthermore, while it is believed that this is the best alternative available to date since the SSL compliant server offers the easiest and most transparent solution to consumers, this scheme does not address the needs of a remote company subscriber. Specifically, this scheme fails to provide a complete and secure solution for a company subscriber without a server on the premises.

Payments using third parties

For payment schemes involving third parties, a company collects and approves all payments from one client to another. All the information necessary for the transaction is collected via the Internet except for the confidential credit card number data. Specifically, the credit card number data is transmitted via a secure telephone line and the information is kept on a secure computer that cannot be accessed from the Internet. (The third party makes money by charging the merchant and consumer for services much in the same way as conventional credit card companies make money.)

For an example of this payment scheme implemented, see First Virtual, NetChex, and the NetBill Project.

While this scheme is simple, safe and highly secure without requiring the use of complicated encryption techniques, there are seen to be a number of disadvantages. In particular, this scheme suffers the disadvantages of adding the cost of third-party services, allowing spending limits to be reached without the knowledge of the consumer since money is linked to a credit card, and the potential loss of privacy since all data is gathered in a centralized system. Furthermore, problems utilizing this scheme also result from the need to manage shipping costs, backorders, delayed shipments, and billing problems arising from the involvement of the third party.

OPEN MARKETS, offers another alternative for providing the merchant with the customer order via a highly developed and dedicated secure server. Specifically, credit card information is handled by OPEN MARKETS, through a dedicated "back-end" server hosted by OPEN MARKETS, which is linked by dedicated phone lines to a financial institution. The credit card information is not processed until OPEN MARKETS is notified by the retailer, via regular e-mail or phone, that the order has been shipped. At that time OPEN MARKETS processes the credit card information for the retailer. However, this scheme also suffers from many of the disadvantageous above-described.

Payments Using Digital Cash

This scheme uses a third party as well but differs significantly from the previously described third party scheme. In the previous third party payment scheme, the third party was analogous to the post office. In the digital cash scheme, the third party acts as a virtual bank that provides "digital coins" to the consumer. In particular, money is deposited via a credit card over secure telephone lines or mailed in the form of a check to the virtual bank in the same manner as a conventional bank account. The consumer can then withdraw the digital coins from their Internet bank account and store them on the hard drive. When a purchase is made, the money is withdrawn from the hard drive and transmitted to the merchant or another party. Smartcards can also be used to store digital coins allowing cash to be carried. The scheme of providing security for the digital coins is again RSA public-key encryption.

Specifically, when utilizing this scheme to make withdrawals from the virtual bank, the consumers PC determines the equivalent digital coin amount required by the user and produces a random serial number representative of said amount. Thereafter, the serial number is "blinded" using RSA public-key cryptography to insure privacy. The bank encodes the serial numbers with its own secret key (digital signature) and debits the consumers account. The digital coins are then sent back to the user and decoded using the banks public key for storage on the consumers PC. To spend the digital coins, the PC collects the amount of coins necessary to reach the requested total value of the transaction which coins are sent to the receiver. The receiver then

sends the coins directly to the digital bank where the bank verifies the validity of the digital coins and credits the account of the receiver.

For an example of this payment scheme implemented, see CyberCash, Digicash, and Net Bank.

While this scheme has the advantages of providing anonymity for the consumer, quickness, and working much on the same familiar principle as cash, this scheme nevertheless suffers the disadvantage of being complicated. In addition, hardware failure can mean loss of money. As a result, this scheme has not gained widespread support from banks and merchants.

A variation to this scheme would be CYBERCASH's "wallet" software. CYBERCASH provides a method for allowing subscribers on a networked communications system to transfer commercial information to a company subscriber in a secured manner. In particular, CYBERCASH requires a subscriber "wallet" which is a piece of software that must be downloaded or otherwise locally installed on the subscriber unit before any commercial transactions may occur. The subscriber then must utilize the "wallet" software to encrypt, specifically PGP encrypt, any information that the subscriber wishes to maintain as secure. This encrypted information is then transferred to a designated server and accordingly forwarded to the company subscriber and CYBERCASH for description. The financial institution is linked via a dedicated phone line to CYBERCASH. The credit card transaction is approved and that data is reencrypted and returned to the subscriber and the company subscriber. The basic drawback to this scheme is primarily the additional software required by the consumer and a complicated back-end system that incorporates a third party, CYBERCASH and a bank, plus several back-and-forth transactions all resulting in numerous file structures. This scheme suffers the further disadvantage of requiring the user to have specialized programming resident on the user's subscriber unit.

From the foregoing description of available secured commercial transaction methods, it is seen that a need exists for an improved method of providing secured commercial transactions via a networked communications system.

As a result of this existing need, it is an object of the present invention to provide a method of providing secured commercial transactions via a networked communications system in which consumers will have confidence.

It is a further object of the invention to provide a method that is easy, attractive, and transparent to consumers when utilized.

It is yet another object of the present invention to ensure that no residue of the commercial transaction is available to authorized network subscribers.

It is still a further object of the present invention to provide a service in which company subscribers can receive secured commercial information in a cost effective manner.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method for providing secured commercial transactions in a networked communications system comprising a client unit, a secured host server, and a company subscriber unit is provided. Generally, the method includes the steps of providing a secured transmission path via the networked communications system between the client unit and the secured host server, receiving encrypted commercial information transmitted via the secured transmission path by the client unit at the secured host server, reencrypting the once encrypted commercial information in response to the step of receiving encrypted commercial information, and forwarding the reencrypted commercial information via the communications network from the secured host server to the company subscriber unit.

More specifically, the method includes the steps of providing a secured transmission path via the networked communications system between the client unit and the secured host server, presenting the client unit with an order form in which commercial information is to be entered via the secured transmission path, receiving the commercial information transmitted via the secured transmission path by the client unit at the secured host server, maintaining the commercial information solely in the dynamic memory of the secured host server, encrypting the commercial information in response to the step of receiving the commercial information, erasing the dynamic memory of the secured host server in response to the step of encrypting the commercial information, and forwarding the encrypted commercial information via the communications network from the secured host server to the company subscriber unit.

A better understanding of the objects, advantages, features, properties and relationships of the invention will be obtained from the following detailed description and accompanying drawing that sets forth an illustrative embodiment and is indicative of the various ways in which the principles of the invention may be employed.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the invention, reference may be had to FIG. 1 which illustrates a communications network on which the subject invention resides.

DETAILED DESCRIPTION

With reference to the figures and Appendix A, a method for providing secured commercial transactions via a networked communications system is disclosed. As will be readily understood by one skilled in the art, the system on which the method resides generally comprises a communications network, such as the internet, which has attached thereto a client unit **10**, a secured host server **12**, and a company subscriber unit **14**. The client unit **10** is preferably a personal computer equipped with appropriate access software such as MICROSOFT EXPLORER, version 2.0+, and NETSCAPE NAVIGATOR, version 1.2+. The secured host server **12** is preferably a NETSCAPE commerce server that utilizes a 128-bit, non-export encryption key that corresponds to the DES standard (UPS Military grade security). The DES keys may be obtained from RSA Data Technologies. It will also be understood that the product or services available to the client will be "advertised" on the communications network by a company subscriber making available an unsecured HTML document which may be part of a local network or remote from the company subscriber unit.

To initiate the ordering of a product or service off the web, the client unit first establishes a Secure Sockets Layer (SSL) session utilizing the above-mentioned access software which transfers the link from an unsecured first server to the secured host server. Thereafter, once the two way, secured, SSL communications link is established between the client unit and the secured host server, the client automatically authenticates the connection via the entering of predetermined certificate keys. This authentication code is passed and confirmed between the client and the secured host server. In this manner, any information passed between the two devices is transferred in a secure, encrypted manner via DES grade encryption.

Once the secure connection has been established via the SSL, the secured host server presents the client unit with an order form to be displayed thereon, typically created in Hypertext Markup Language (HTML), which includes various information fields which the user must complete in order to proceed with the commercial transaction. It is contemplated that among these various information fields will be a field that will require the user to enter personal details, credit card information, and a list of the products/services that are desired. After the pertinent information has been entered into the order form, the user causes the information to be transmitted from the client unit to the secured host server. More specifically, the information entered into the information fields of the order form is sent directly to the port and process currently running on the secured host server via the SSL.

In response to the receipt of the information that has been entered into the order form by the client, the secured host server causes the running of a separate sessions program that takes the information submitted thereto and immediately encrypts it with the company subscriber unit PGP public key. More specifically, the information transmitted from the subscriber unit is first and automatically turned into an ASCII text format by the software resident on the secured host server and then "piped" by a perl script to the PGP program and encrypted. It is preferred that each transaction spawn its own individual, separate session. Furthermore, during the PGP encryption process, the information received from the client unit is prevented from being written to disk or otherwise stored or transmitted anywhere on the local network to which the secured host server may be attached. Accordingly, the information received from the client is processed only in the high or dynamic random access memory (RAM) of the secured host server upon its receipt. Once the information has been encrypted utilizing the company subscriber unit PGP public key, the dynamic memory of the secured host server that contains the information transmitted via the SSL is erased or otherwise overwritten.

It will be appreciated by those skilled in the art that this process of PGP encrypting occurs in nanoseconds. Accordingly, the information transferred via the SSL from the client unit to the secured host server never resides on the secured host server for any significant duration of time. In this manner, the information transferred via the SSL is, for all practical purposes, never resident on the communications network or secured host server where said information would be capable of being accessed by a hacker or any other unauthorized network user.

Once the information has been encrypted utilizing the company subscriber unit PGP public key, the company subscriber unit is notified of the transaction and the PGP encrypted information is transferred thereto for processing. The transfer of the PGP encrypted information is preferably accomplished through sending the PGP encrypted information to the company subscriber unit via electronic-mail or the like. Additionally, at the close of the perl script, it is preferred that an acknowledgment be automatically generated in the form of an unencrypted e-mail and returned to the client unit. This acknowledgement should include a copy of the order minus the credit card data and other data the company subscriber feels need not be transmitted. While not necessary, local copies of the PGP encrypted information may also be submitted to a special, unannounced server that is provided as a simple backup. An unannounced server is equipped with a one-way gate and any information stored therein is inaccessible by third parties connected to the network.

Once the company subscriber has downloaded the PGP encrypted information, any residue thereof which may reside on the E-mail server will be overwritten during the normal course of its operation. At this point, an authorized agent of the company subscriber will authenticate the PGP encrypted e-mail and, thereafter, take the PGP encrypted information and run it through a decryption program provided by the operator of the secured host server. Any tampering of the PGP secured transaction will be noticeable in the authentication process. (See the documents attached to Appendix A showing the PGP encrypted order (1) and the decrypted order (2) noting the date, time, and invoice number stamps on both the decrypted order (2) and the subscriber acknowledgment (3)).

The decryption program will require the company subscriber unit's private key and key phrase to confirm and continue the decryption process. If the appropriate key-generated key code is submitted, the PGP encrypted information is decrypted and the company subscriber may thereafter process the information in its regular course of business. From the preceding description, it will be apparent that the invention overcomes the problems associated with the prior art in that there is no residual, centralized file structure which is exposed to attack, the management of billing issues resides with the retail subscriber, the operating costs are reduced, and the encryption scheme is transparent to the consumer and the retailer. Furthermore, since the retailer receives the private key while the operator of the secured host server maintains the public key, transactions are even secure from the operator of the secured host server. In sum, the described invention has the advantages of providing a user friendly, user transparent, and highly secure method of performing commercial transactions via a communications network.

While specific embodiments of the invention have been described in detail, it will be appreciated by those skilled in the art that various modifications and alternatives to those details could be developed in light of the overall teachings of the disclosure. Accordingly, the particular arrangements disclosed are meant to be illustrative only and not limiting as to the scope of the invention that is to be given the full breadth of the appended claims and any equivalent thereof.

APPENDIX A

The following perl script is utilized to encrypt and mail, by PGPMAIL, information submitted using a CGI form script.

```
#!/usr/bin/perl
#Gregory Luneau, Greg@Solutions.Net
#Copyright (c) 1995, 1996
#Process the input from POST method of the HTML page.
$buffer = <STDIN>;
```

APPENDIX A-continued

```
@pairs = split(/&/,$buffer);
foreach $pair (@pairs)

{
($tag, $value) = split(/=/, $pair);
$value =~tr/+//;
$value =~s/%([a-fA-F0-9] [a-fA-F0-9])/pack("C", hex($1))/eg;
$FORM{$tag} = $value;
}

#Tells the PGP program where the public key chain is.
$ENV{"PGPPATH"} = "/html/company/.pgp/";
#This will encript everything sent to PGPMAIL with PGP,
#and then Mail it to the Company Subscriber Unit with Mail.
local($pid) =open(PGPMAIL,"|/usr/bin/pgp+batchmode+verbose =0 -fate
company |/usr/sbin/Mail -s'A Transaction from the Net'
company@unit.com");
print PGPMAIL "Name: $FORM{CLIENT}\n";
print PGPMAIL "Credit Card: $FORM{ccnumber}\n";
#. . .more information could be sent from here, ex: expiration date,
# list of products, etc.

# After this instruction, the whole PGPMAIL process executes and then
# terminates.
close(PGPMAIL);

#Tells the Client unit what happened
print "Content-type: text/html\n\n";
print "<HTML><BODY><H1>\n";
print "The Transaction has been transmitted securely.\n";
print "</H1></BODY></HTML>\n";

#Memory cleans up happens after the script ends.
```

Date. 96-04-23 11:26:50 EDT
From: http@mail2.digimark.net (HTTP User)
To: kinghill1@aol.com

```
------BEGIN PGP MESSAGE------
Version: 2.6

hEwClnFEqjelEmkBAf92ds4E4vmd40GZUdzb6iIvBjIrOU6zn/4DjnsSxokomi4p
g4FNSDxcCvZ7scoURAov7MFEQ7uovv+7b0nmtJcFpgAAAc01aFyUnfU9L7W2c0qP
AZOgWS8Fr45r0AeLq/Mv4FNUkEAAmKiNtab8xhYnYc+xVHjmY1AKZJlEEMUoy4aU
gCNmen/AMc3MDGjytAF1XSWX1YFprH9c7CjZ+RvOSbQ5RGjj9AY88YUmpDYsGekK
DxA51QLMB5TXKDw7K9mP3bc/vWI5pPdzPrHwxSuoLSLupECVD7IUqvvRSCNmcyxG
0QoGAF9HPosTrT7w8H6ksR5VwLIEVWZ5QTz8/J5983AqH+0Gf+zkM6ZaUh+a1mHC
Te24eNwXzq/Vc5vgyZBiWwOf5db3nUAg/KnryYmTqjBcdNpDi6ZHeDt3MajPvPW9
hBtDsuhRcFKQmQlED76mjvrkvMwUYf118MqoamJnclbUpPVeL4hpBugTjRznixwA
cGzjK5IDY2f1UcEAuJ43tbOthrSyX3Y9+Ctar3LR2s8JdB2Qsl+h1Axw1yDWaNdG
WXLGxuIdX6u4sVbZpkiDIlWdn/Dx/0FPL3iPWJmgogKTXb7d4IMTDHuzkBSAaKwL
fYI4SBlOCuHa5MCG72KcND+Ua4wc4zTMChOtrIVuH4kY9Eue5rRgFtDjmBH48nRH
fbV9yvbDP57sdjZT94k5vg==
=lPdL
-------END PGP MESSAGE-----
```

```
----------Headers----------
From http@mail2.digimark.net  Tue Apr 23 11:26:36 1996
Return-Path: http@mail2.digimark.net
Received: from polyhymnia.digimark.net  (polyhymnia.digimark.net [198.77.86.8])
by emin22.mail.aol.com (8.6.12/8.6.12) with ESMTP id LAA29954 for
<kinghill1@aol.com>; Tue, 23 Apr 1996 11:26:35 -0400
Received: from urania.digimark.net  (urania.digimark.net [198.77.86.7]) by
polyhymnia.digimark.net (8.7.5/8.7.3) with ESMTP id LAA17714 for
<kinghill1@aol.com>; Tue, 23 Apr 1996 11:26:57 -0400 (EDT)
Received: (from http@localhost) by urania.digimark.net (8.7.5/8.7.3) id
LAA10417 for kinghill1@aol.com; Tue, 23 Apr 1996 11:26:30 -0400 (EDT)
Date: Tue, 23 Apr 1996 11:26:30 -0400 (EDT)
From: HTTP User <http@mail2.digimark.net>
Message-Id: <199604231526.LAA10417@urania.digimark.net>
To: kinghill1@aol.com
Subject: Invoice to Tom King from King of the Hill
```

APPENDIX A-continued

4-23-1996 America Online:Kinghill1 Page 1

Thank you Tom King for Ordering with us.

Name:	Tom King
Address:	P.O. Box 304
City/Town:	Addison
Province/State:	IL
Country:	USA
Postal/Zip Code:	60101-0304
Telephone:	708-279-5550
Fax:	708-279-5572
Email:	ThomasK797@aol.com
Credit Card:	Master Card
Card Numher:	4444 4444 4444 4444
Expiriation Date:	01/97

Order Code:	Short Description:	# of Unit(s):	Unit Price:
	#5 Teton Fly Reel	1	$175.00

SubTotal: $ 175.00
Freight to All other countries: $ 10.00
plus Illinois Taxe (6.5%): $ 12.03
Total: $ 197.03

Date: 23/4/96
Time: 11:26
Invoice: 51

Date: 96-04-23 11:26:42 EDT
From: http@mail2.digimark.net (HTTP User)
To: ThomasK797@aol.com

Thank you Tom King for Ordering with us.

You are being billed for the following amount.

Total: $ 197.03

Date: 23/4/96
Time: 11:26
Invoice: 51

----------Headers----------
From http@mail2.digimark.net Tue Apr 23 11:26:35 1996
Return-Path: http@mail2.digimark.net
Received: from polyhymnia.digimark.net (polyhymnia.digimark.net [198.77.86.8])
by emin20.mail.aol.com (8.6.12/8.6.12) with ESMTP id LAA23538 for
<ThomasK797@aol.com>; Tue, 23 Apr 1996 11:26:35 -0400
Received: from urania.digimark.net (urania.digimark.net [198.77.86.7]) by
polyhymnia.digimark.net (8.7.5/8.7.3) with ESMTP id LA17712 for
<ThomasK797@aol.com>; Tue, 23 Apr 1996 11:26:57 -0400 (EDT)
Received: (from http@localhost) by urania.digimark.net (8.7.5/8.7.3) id
LAA10416 for ThomasK797@aol.com; Tue, 23 Apr 1996 11:26:29 -0400 (EDT)
Date: Tue, 23 Apr 1996 11:26:29 -0400 (EDT)
From: HTTP User <http@mail2.digimark.net>
Message-Id: <199604231526.LAA10416@urania.digimark.net>
To: ThomasK797@aol.com
Subject: Invoice to Tom King from King of the Hill

4-23-1996 America Online:ThomasK797 Page 1

What is claimed is:

1. In a networked communications system comprising a client unit, a secured host server, and a company subscriber unit, a method for providing secured commercial transactions via the networked communications system comprises the steps of:

providing a secured transaction path via the networked communications system between the client unit and the secured host server;

receiving encrypted commercial information transmitted via the secured transmission path by the client unit at the secured host server;

reencrypting substantially all of the once encrypted commercial information in response to the step of receiving encrypted commercial information; and

forwarding the reencrypted commercial information via the communications network from the secured host server to the company subscriber unit.

2. The method as recited in claim **1**, further comprising the steps of maintaining the encrypted commercial information solely in the dynamic memory of the secured host server and erasing the dynamic memory of the secured host server in response to the step of reencrypting the encrypted commercial information.

3. The method as recited in claim **2**, wherein the step of providing a secured transmission path comprises the step of establishing a Secured Sockets Layer (SSL).

4. The method as recited in claim **1**, wherein the step of reencrypting substantially all of the once encrypted commercial information further comprises the step of PGP encrypting the encrypted commercial information.

5. The method as recited in claim **3**, further comprising the step of presenting the client unit with an order form having information fields and utilizing the secured sockets layer to encrypt commercial information entered into the information fields.

6. In a networked communications system comprising a client unit, a secured host server, and a company subscriber unit, a method for providing secured commercial transactions via the networked communications system comprising the steps of:

providing a secured sockets layer transmission path via the networked communications system between the client unit and the secured host server;

presenting the client unit with an order form in which commercial information is to be entered via the secured socket layer transmission path;

receiving the commercial information transmitted via the secured sockets layer transmission path by the client unit at the secured host server;

maintaining the commercial information solely in the dynamic memory of the secured host server;

PGP encrypting the commercial information in response to the step of receiving the commercial information;

erasing the dynamic memory of the secured host server in response to the step of PGP encrypting the commercial information; and

forwarding the PGP encrypted commercial information via the communications network from the secured host server to the company subscriber unit.

7. The method as recited in claim **6**, wherein the step of forwarding the PGP encrypted commercial information includes the step of:

utilizing unsecured commercial electronic mail.

8. The method as recited in claim 1 wherein the step of forwarding the re-encrypted commercial information includes the step of

utilizing unsecured commercial electronic mail.

* * * * *

US005751813A

United States Patent [19]

Dorenbos

[11] Patent Number: 5,751,813

[45] Date of Patent: May 12, 1998

[54] **USE OF AN ENCRYPTION SERVER FOR ENCRYPTING MESSAGES**

[75] Inventor: **David Dorenbos**, Elmhurst, Ill.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **639,457**

[22] Filed: **Apr. 29, 1996**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/49**; 380/25

[58] **Field of Search** 380/49, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

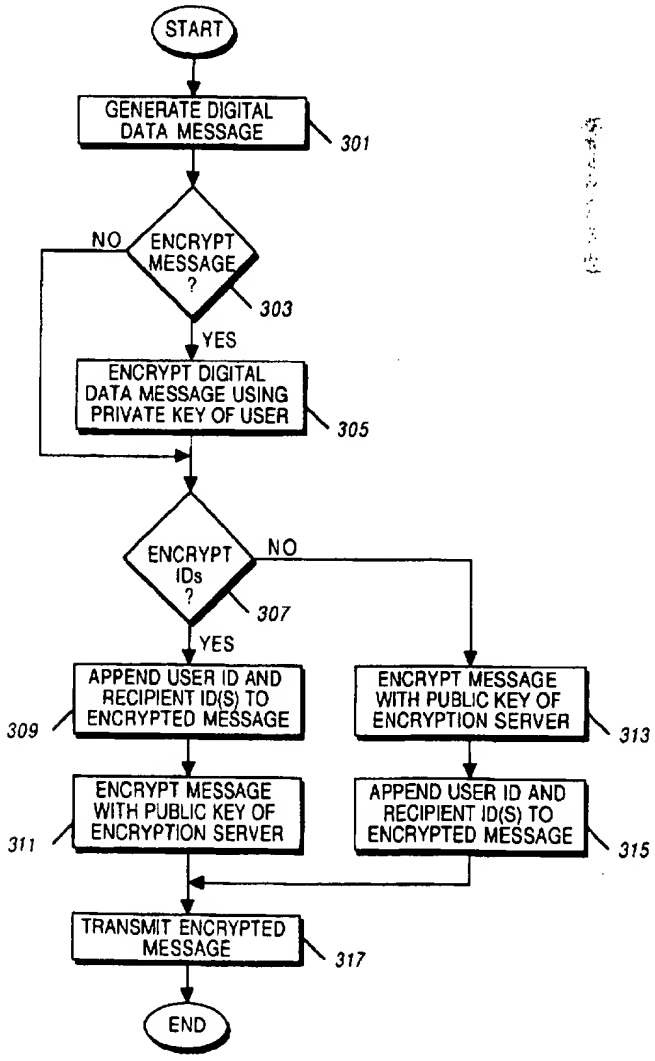
5,455,865	10/1995	Perlman	380/49
5,479,514	12/1995	Klonowski	380/47
5,574,785	11/1996	Ueno	380/2

Primary Examiner—Thomas H. Tarcza
Assistant Examiner—Carmen D. White
Attorney, Agent, or Firm—Susan L. Lukasik

[57] **ABSTRACT**

An encryption server receives a first encrypted message (**105**) and decrypts (**403**) the encrypted message using a first key, yielding a decrypted message comprising a second encrypted message (**105A**), an identification of a sender of the first encrypted message, and an identification of a first recipient. The second encrypted message, the identification of the sender, and the identification of the first recipient are determined (**405**) from the decrypted message. The second encrypted message and the identification of the sender are encrypted (**409**) with a second key, yielding a third encrypted message (**109**). The third encrypted message (**109**) is transmitted to the first recipient.

34 Claims, 4 Drawing Sheets



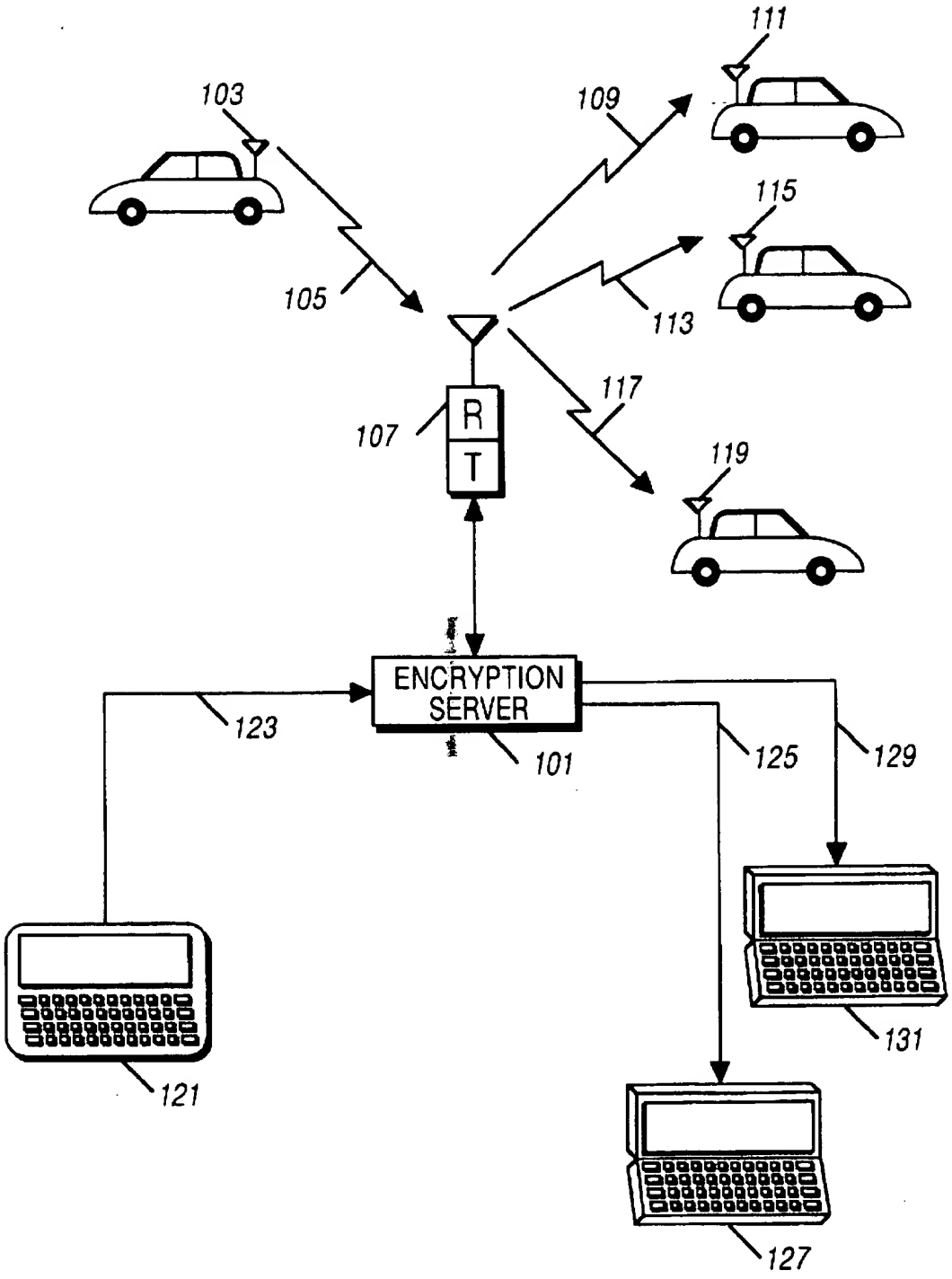

111
103
109
115
105
113
R
T
107
117
119
ENCRYPTION SERVER
123
101
125
129
121
131
127

FIG. 1

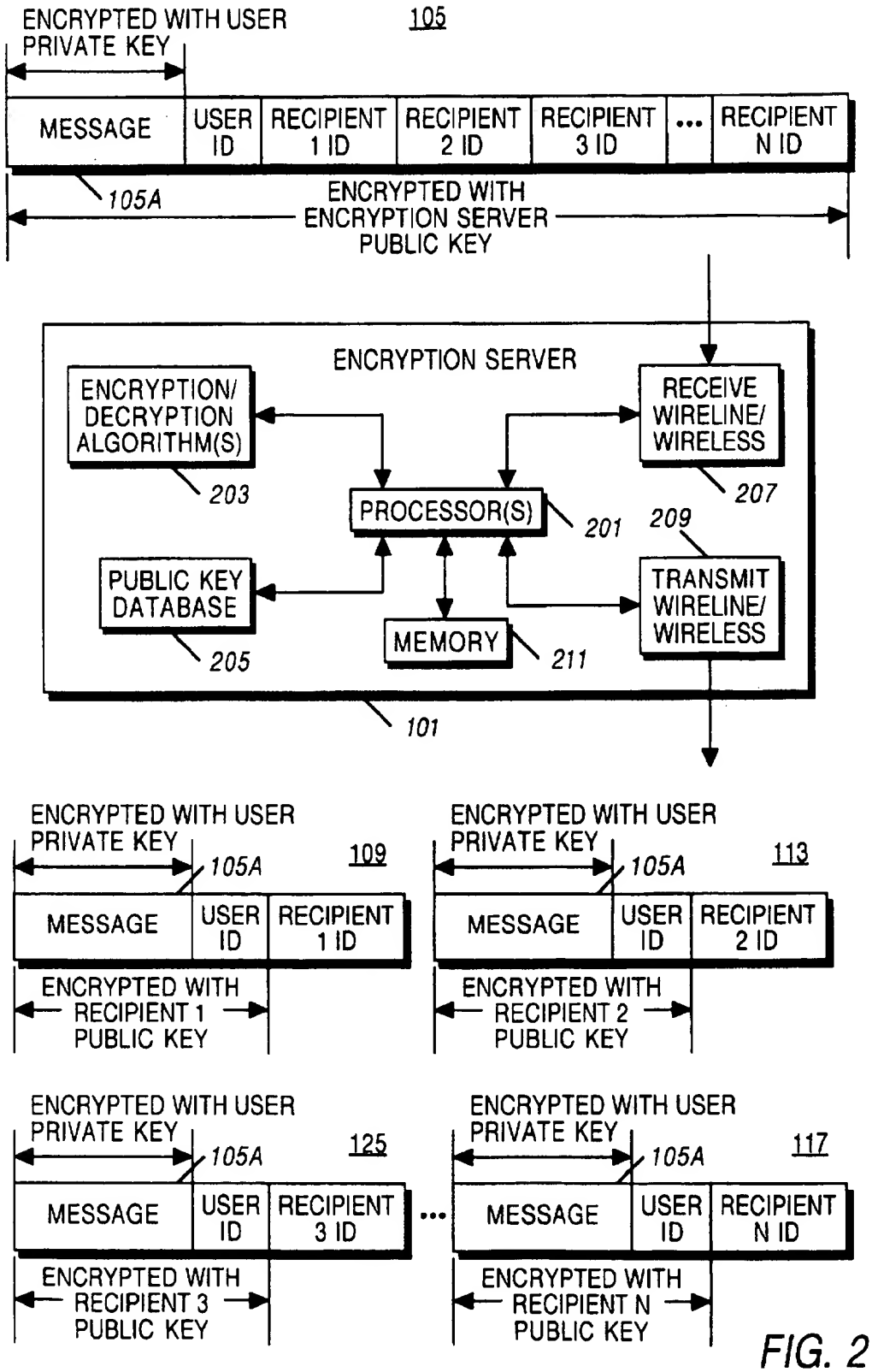

ENCRYPTED WITH USER PRIVATE KEY
105
MESSAGE
USER ID
RECIPIENT 1 ID
RECIPIENT 2 ID
RECIPIENT 3 ID
...
RECIPIENT N ID
105A
ENCRYPTED WITH ENCRYPTION SERVER PUBLIC KEY
ENCRYPTION SERVER
ENCRYPTION/ DECRYPTION ALGORITHM(S)
203
RECEIVE WIRELINE/ WIRELESS
207
PROCESSOR(S)
201
209
PUBLIC KEY DATABASE
205
TRANSMIT WIRELINE/ WIRELESS
MEMORY
211
101
ENCRYPTED WITH USER PRIVATE KEY
105A
109
MESSAGE
USER ID
RECIPIENT 1 ID
ENCRYPTED WITH RECIPIENT 1 PUBLIC KEY
ENCRYPTED WITH USER PRIVATE KEY
105A
113
MESSAGE
USER ID
RECIPIENT 2 ID
ENCRYPTED WITH RECIPIENT 2 PUBLIC KEY
ENCRYPTED WITH USER PRIVATE KEY
105A
125
MESSAGE
USER ID
RECIPIENT 3 ID
ENCRYPTED WITH RECIPIENT 3 PUBLIC KEY
...
ENCRYPTED WITH USER PRIVATE KEY
105A
117
MESSAGE
USER ID
RECIPIENT N ID
ENCRYPTED WITH RECIPIENT N PUBLIC KEY

FIG. 2

FIG. 3

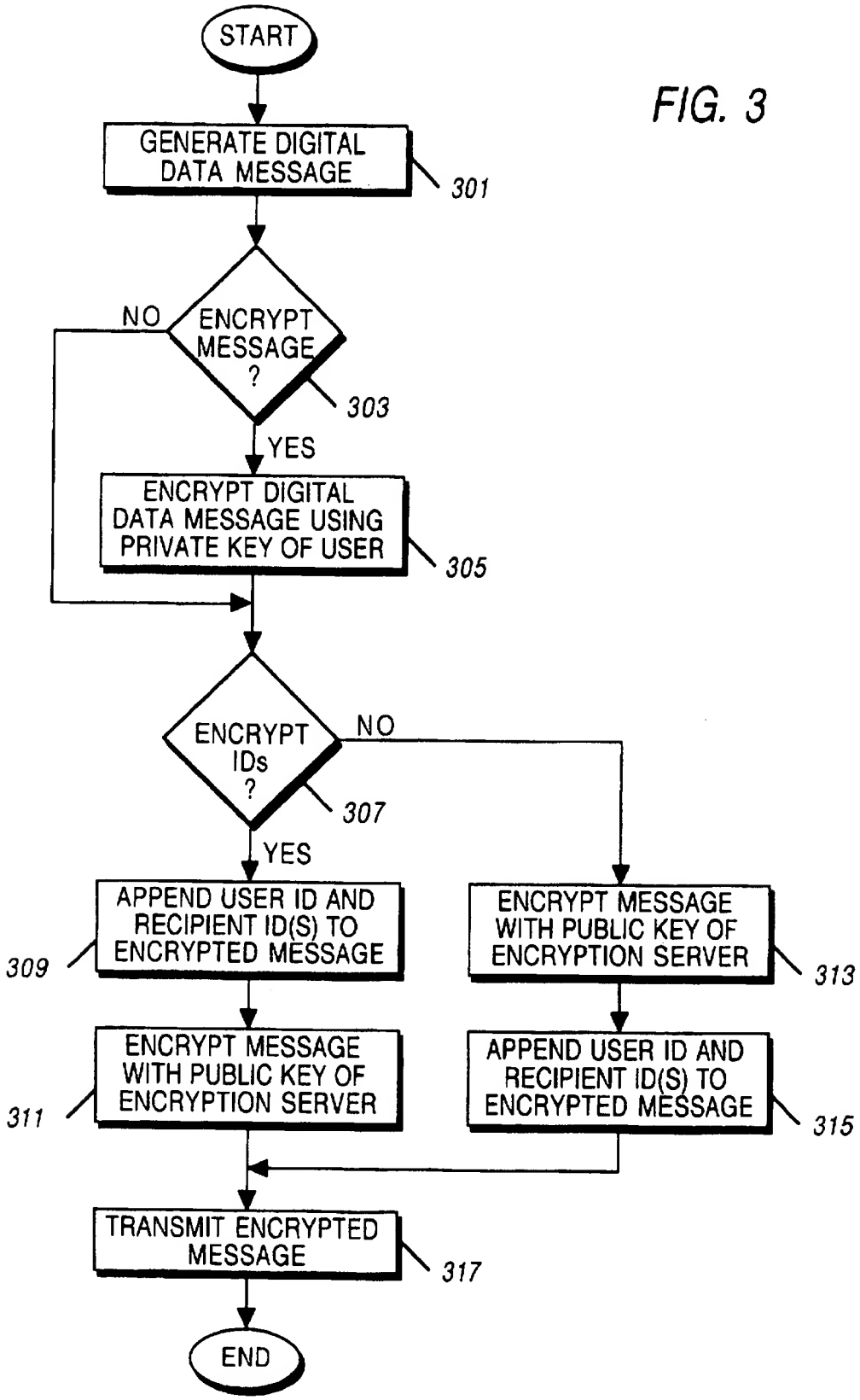
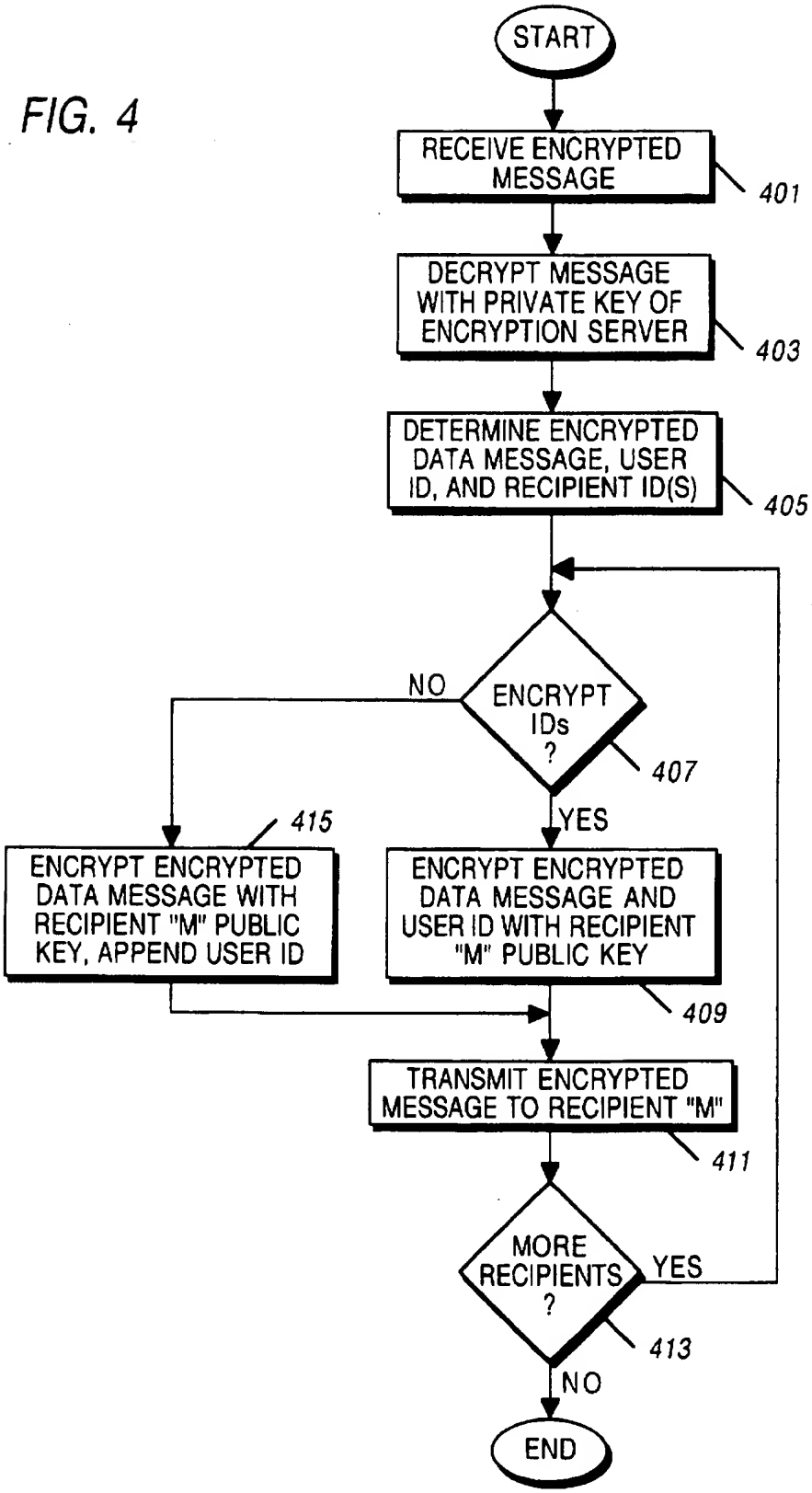

START
GENERATE DIGITAL DATA MESSAGE
301
ENCRYPT MESSAGE ?
NO
303
YES
ENCRYPT DIGITAL DATA MESSAGE USING PRIVATE KEY OF USER
305
ENCRYPT IDs ?
NO
307
YES
APPEND USER ID AND RECIPIENT ID(S) TO ENCRYPTED MESSAGE
309
ENCRYPT MESSAGE WITH PUBLIC KEY OF ENCRYPTION SERVER
311
ENCRYPT MESSAGE WITH PUBLIC KEY OF ENCRYPTION SERVER
313
APPEND USER ID AND RECIPIENT ID(S) TO ENCRYPTED MESSAGE
315
TRANSMIT ENCRYPTED MESSAGE
317
END

FIG. 4


START
RECEIVE ENCRYPTED MESSAGE
401
DECRYPT MESSAGE WITH PRIVATE KEY OF ENCRYPTION SERVER
403
DETERMINE ENCRYPTED DATA MESSAGE, USER ID, AND RECIPIENT ID(S)
405
ENCRYPT IDs ?
407
NO
YES
415
ENCRYPT ENCRYPTED DATA MESSAGE WITH RECIPIENT "M" PUBLIC KEY, APPEND USER ID
ENCRYPT ENCRYPTED DATA MESSAGE AND USER ID WITH RECIPIENT "M" PUBLIC KEY
409
TRANSMIT ENCRYPTED MESSAGE TO RECIPIENT "M"
411
MORE RECIPIENTS ?
413
YES
NO
END

USE OF AN ENCRYPTION SERVER FOR ENCRYPTING MESSAGES

FIELD OF THE INVENTION

This invention relates to communication systems, including but not limited to encrypted communication systems.

BACKGROUND OF THE INVENTION

Encrypted voice and data communication systems are well known. Many of these systems provide secure communications between two or more users by sharing one or more pieces of information between the users, which permits only those users knowing that information to properly decrypt the message. This information is known as the encryption key, or key for short. Encryption keys may be private keys, where a single key is utilized for encryption and decryption, or public keys, where multiple keys are utilized for encryption and decryption.

Methods of encrypting using public-key encryption are well known in the art. Typically, a public-key encryption is a method of encryption by which a single message is encrypted using a sender's private key and then a recipient's public key. The recipient then decrypts the message using the recipient's private key and then the sender's public key. Typically, public keys are 512 bits long, although some public keys have as few as 256 bits. Some encryption experts recommend using 1024-bit keys. Because the computational power required to break a key increases exponentially with the length of the key, longer keys provide more security. In addition, because two keys are needed to decrypt a message, two longer keys are more difficult to decrypt if neither key is known.

Today, secure communication systems are used to transmit data in an encrypted fashion. If a user wishes to send the same message to five different recipients, the user must encrypt the message five different times, each time using the public key of a different recipient for the message. The user then transmits the five messages to the five recipients. Such a process, however, is troublesome when the user wishes to transmit to, for example, 100 or more recipients. In this instance, the user must encrypt each message individually 100 or more times, one for each recipient. If the user has a portable communication device, such as a laptop computer, the user's battery may run out of power before encryption and transmission of each message has occurred. In addition, the encryption and transmission process can consume a lot of time and processing power for the portable device, rendering the portable device unavailable for other activities by the user during the encryption and transmission time period. Thus, such transmissions would be impractical for portable users.

Accordingly, there is a need for a method of transmitting encrypted data messages to multiple users without resulting in a time or power barrier to the user's communication device.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a communication system having an encryption server in accordance with the invention.

FIG. 2 is a block diagram of an encryption server in accordance with the invention.

FIG. 3 is a flowchart showing a method of transmission of a digital data message to an encryption server in accordance with the invention.

FIG. 4 is a flowchart showing a method of transmission of an encrypted message by an encryption server in accordance with the invention.

DESCRIPTION OF A PREFERRED EMBODIMENT

The following describes an apparatus for and method of using an encryption server for encrypting messages. Messages are encrypted twice, once with the sender's private key and then with an encryption server's public key before transmission of the messages to the encryption server. The encryption server decrypts received messages with the encryption server's private key, yielding an encrypted message, a user identification (ID), and one or more recipient IDs. The encryption server encrypts the encrypted message and the user ID individually with each of the recipient's public keys and transmits the resultant message(s) to the appropriate recipient. Each recipient decrypts the messages using the recipient's private key and the sender's public key. A secure communication system is thereby provided, wherein portable communication devices are neither tied up nor drained of power because the device's user wishes to send a single encrypted message to multiple recipients.

A method of using an encryption server for encrypting messages comprises the steps of, at a communication unit operated by a user generating a digital data message, The digital data message is encrypted using a first key, yielding a first encrypted message. An identification of the user and an identification of a first recipient are appended to the first encrypted message, yielding an appended first encrypted message. The appended first encrypted message is encrypted using a second key, yielding a second encrypted message. The second encrypted message is transmitted to an encryption server. At the encryption server, the second encrypted message is received. The second encrypted message is decrypted using a third key, yielding the appended first encrypted message. The first encrypted message, the identification of the user, and the identification of the first recipient are determined from the appended first encrypted message. The first encrypted message and the identification of the user are encrypted with a fourth key, yielding a third encrypted message. The third encrypted message is transmitted to the first recipient. In the preferred embodiment, the first key is a private key associated with the user, the second key is a public key associated with the encryption server, the third key is a private key associated with the encryption server, and the fourth key is a public key associated with the first recipient. Alternatively, the second key and the third key may be identical. The transmitting steps may be performed over wireless communication resources, such as radio frequency communication resources, or wireline communication resources, such as standard telephone lines or fiber optic cable.

In addition, the step of appending may further comprise the step of appending an identification of a second recipient to the first encrypted message, thereby yielding the appended first encrypted message. In this case, the method further comprises the steps of encrypting, by the encryption server, the first encrypted message and the identification of the user with a fifth key, yielding a fourth encrypted message, and transmitting the fourth encrypted message to the second recipient. In the preferred embodiment, the fifth key is a public key associated with the second recipient. Alternatively, the step of appending may comprise the step of appending three or more identifications of recipients to the first encrypted message, thereby yielding the appended first encrypted message.

A block diagram of a communication system having an encryption server is shown in FIG. 1. An encryption server **101** is shown at the center of FIG. 1. Further details of the encryption server **101** are shown in FIG. 2 described below. A user of a first communication unit **103** utilizes the first communication unit **103** to generate an digital data message that is encrypted in two stages in the preferred embodiment. In the first stage, the digital data message is encrypted using a first key, which is the user's private key in the preferred embodiment. The result of this encryption is a first-stage encrypted message. (In an alternate embodiment, the digital data message is not encrypted using the first key.) The user's identification (ID) and one or more recipient IDs are appended to the first-stage encrypted message, yielding an appended message. The appended message is encrypted using a second key, yielding a second-stage encrypted message **105**. In the preferred embodiment, the second key is the public key associated with the encryption server **101**. The communication unit transmits the second-stage encrypted message **105** to the encryption server via a wireless communication link to a wireless communication device **107**, such as a radio frequency (RF) base station, repeater, or radio, or infrared communication device. The second-stage encrypted message **105** is conveyed by the wireless communication device **107** to the encryption server **101**.

The encryption server **101** decrypts the second-stage encrypted message **105** using an appropriate key. In the preferred embodiment, the appropriate key is the encryption server's private key. The encryption server **101** then determines the user's ID from the decrypted message and also determines the IDs of all recipients that the user indicated as intended targets of the first-stage encrypted message. The encryption server **101** then encrypts the user's ID along with the first-stage encrypted message by encrypting with the public key of the first recipient. The resultant message **109** is transmitted to the first recipient, who utilizes communication unit **111**. The encryption server then encrypts the first-stage encrypted message along with the user's ID by encrypting with the public key of the second recipient and transmitting the resultant encrypted message **113** to the second recipient, who utilizes communication unit **115**. This process continues until the encryption server reaches the last recipient ID on the user's list, and encrypts the first-stage encrypted message along with the user's ID by encrypting with the public key of the last recipient and transmitting the resultant encrypted message **117** to the last recipient, who utilizes communication unit **119**.

The encryption server **101** may also receive user requests for encryption from wireline communication devices **121** via wireline channels. As with the wireless transmission, the encryption server decrypts the received message **123** using the private key of the encryption server, then encrypts the resultant message individually for each different recipient using the appropriate recipient's individual public key. These recipients may be wireline devices **127** and **131**, which receive the messages **125** and **129** via wireline communication channels.

The above examples describe RF to RF transmission and wireline to wireline transmission of encrypted messages. Nevertheless, the method of the present invention is equally successful if a wireline device **121** requests transmission to wireless communication units **111**, **115**, and **119**. Similarly, a wireless communication unit **103** may request transmission from the encryption server **101** to wireline communication devices **127** and **131**. In addition, the recipients may be a combination of both wireless and wireline communication units **111**, **115**, **119**, **127**, and **131**, regardless of whether the sender uses a wireless communication unit **103** or a wireline communication device **121**.

Upon receipt of the encrypted message from the encryption server, each recipient decrypts the message with the recipient's own private key, and after determining the user's ID, decrypts the resultant message with the user's public key, thereby yielding the original digital data message. The user is also referred to as the sender of the (second-stage) encrypted message **105**.

A block diagram of an encryption server **101**, including its input signals **105** and output signals **109**, **113**, **125**, and **117**, is shown in FIG. 2. In the preferred embodiment, the encryption server **101** is a Sun SparcServer2000 in a multiprocessor configuration, available from Sun Microsystems. The encryption server **101** comprises one or more processors **201**, such as microprocessors or digital signal processors, as are well known in the art. The processors **201** have access to encryption and decryption algorithm(s) **203**, a public key data base **205**, and memory **211**. The encryption/decryption algorithms **203** include public key algorithms, private algorithms, and other algorithms as may be used in the art. The public key data base **205** includes a list of IDs, as used by senders (users) and recipients, and the public keys associated with each of these IDs. The memory **211** includes programming and other data as is necessary to provide functionality as described herein for the encryption server **101**. A receive block for wireline and wireless communications **207** and a transmit block for wireline and wireless communications **209** are also connected to the processors **201**. The receive block for wireline and wireless communications **207** performs appropriate demodulation techniques on received messages **105** and **123**. The transmit block for wireline and wireless communications **209** performs appropriate modulation techniques on messages **109**, **113**, **124**, and **117** to be transmitted. In addition, the encryption server **101** may be equipped with hardware and/or software to provide the encryption server **101** with over-the-air-rekeying capabilities.

As shown in FIG. 2, a user message **105** comprises a second-stage encrypted (encrypted using the encryption server's public key) message comprising the digital data message **105A**, first-stage encrypted with the user's (sender's) private key, in addition to the user ID and a number of recipient IDs. Alternatively, the user message **105** may comprise an unencrypted digital data message **105A**, the user ID, and one or more recipient IDs. The user message **105** is input to the receive wireline/wireless block **207**, the output of which is input to the processor(s) **201**. The processor(s) **201** utilize(s) the encryption/decryption algorithm(s) **203** and the public key data base **205** to decrypt the message **105** using the private key of the encryption server. The processor(s) **201** then determine(s) the first-stage encrypted message **105A**, the user ID, and the first recipient ID from the decrypted message. The processor(s) **201** then determine(s) the first recipient's public key from public key data base **205**, and the encrypt the first-stage encrypted message **105A** and the user ID by using the encryption/decryption algorithms **203** and the first recipient's public key. The processor(s) **201** then append(s) the first recipient ID, thereby yielding a message **109** that is sent to the transmit wireline/wireless block **209** for transmitting to the first recipient's communication unit **111**, as shown in FIG. 1. A similar process is performed on the first-stage encrypted message (or unencrypted digital data message) **105A** and the user ID for each of the recipients listed in the user's message **105**.

In an alternate embodiment, the encryption server **101** may be physically distributed as one or more encryption servers. In this embodiment, the encryption server **101** encrypts the message using a second set of private and public keys associated with a second server. The message so encrypted is transmitted to the second encryption server. The second server decrypts the message and then encrypts the message using the public key(s) of the recipient(s). When traffic is heavy, the encryption server **101** may optimize its efficiency by determining the computation required to transmit directly to each recipient or transmit the request to one or more distributed servers. This process is transparent to the user.

The flowchart of FIG. **3** shows a method for use by a communication unit in transmitting a digital data message to an encryption server **101**. At step **301**, a digital data message is generated. If at step **303** the digital data message is not to be encrypted, the process continues with step **307**. If at step **303** the digital data message is to be encrypted, the process continues with step **305**, where the digital data message is encrypted using the private-key of the user who wishes to communicate the message. At step **307**, it is determined if the IDs of the user and/or recipient(s) are to be encrypted. If the IDs are to be encrypted, the process continues with step **309**, where the user ID and recipient ID(s) are appended to the encrypted message from step **305** or the unencrypted message from step **301** if no encryption took place. At step **311**, the message from step **309**, including the appended IDs, is encrypted using the public key of the encryption server **101**. The process continues with step **317**, where the encrypted message is transmitted to the encryption server **101**. If at step **307** the IDs are not to be encrypted, the process continues with step **313**, where the encrypted message of step **305** (or the unencrypted message from step **301** if no encryption took place) is encrypted with the public key of the encryption server **101**. At step **315**, the user ID and recipient ID(s) are appended to the encrypted message of step **313**, and the process continues with step **317**.

In an alternative embodiment, i.e., when the digital data message is not to be encrypted at step **303** of FIG. **3**, the sender or user may decrypt the digital data message and, if desired, the recipient IDs only once, using the encryption server's public key. The encryption server then decrypts the message using the encryption server's private key, and encrypts the message individually for each of the recipients with the recipient's public key. The recipient then decrypts the message using only the recipient's private key. This method requires the user to locally store only one public key, the key of the encryption server. With this method, a single symmetrical key may be used to encrypt and decrypt the messages between the user and the encryption server **101**, and one or more keys may be used to encrypt the messages between the encryption server and the recipient. Nevertheless, for better security, the encryption server **101** engaged in this embodiment should be a physically secured, e.g., locked away with limited access, because unencrypted information is present inside the encryption server **101**. An advantage of such a system includes enabling law enforcement officials the ability to read the decrypted message as available in the encryption server **101**.

The flowchart of FIG. **4** shows the method performed by the encryption server **101** in accordance with the present invention. At step **401**, the encryption server receives the encrypted message transmitted by the communication unit **103**. At step **403**, the encryption server decrypts the message received at step **401** with the private key of the encryption server **101**. At step **405**, the encryption server determines the user ID, the recipient ID(s), and the encrypted (generated at step **305** of FIG. **3**) or unencrypted (generated at step **301** of FIG. **3**) data message. In an alternate embodiment, the encryption server **101** may be equipped with the appropriate keys to decrypt the digital data message **105A** (when the message **105A** is encrypted) so that law enforcement agencies may have full access to all information transmitted in the system.

At step **407**, it is determined if the IDs (i.e., the user ID and/or recipient ID(s)) are to be encrypted before transmission. If the IDs are to be encrypted, the process continues with step **409**, where the encryption server encrypts the encrypted data message along with the user ID, and the recipient's ID if desired, with the recipient's public key. At step **411**, the encryption server transmits the encrypted message to the recipient whose public key was used at step **409**. If at step **413** there are more recipients identified by the user to which the encryption server has not yet encrypted and transmitted the message, the process continues with step **407**. If there are no more recipients at step **413**, the process ends. If at step **407**, the IDs are not to be encrypted, the process continues with step **415**, where the encrypted data message is encrypted with the recipient's public key, and the user ID and the recipient's ID are appended to that encrypted message without further encryption, and the process continues with step **411**.

Optionally, all messages may be encrypted at one time, and then transmitted in succession at one time, rather than encrypting a first message with one public key, then transmitting the encrypted first message right away, then encrypting a second message using another public key, and transmitting the encrypted second message immediately, and so forth.

The above text and associated drawings describe a method using public-key encryption. Private-key encryption, where the same key is used to encrypt and decrypt a message, may also be used. For example, the key used to encrypt the message send to the encryption server may be the same or identical key used to decrypt the encrypted message at the encryption server. In addition, the encryption method employed by the user to encrypt the original digital data message **105A** may also be private-key encryption, rather than public-key encryption. In addition, a different encryption algorithm may be utilized for the user's first stage of encryption than for the user's second stage of encryption, the result of which is transmitted to the encryption server.

In the above manner, the encryption server encrypts the user's data message individually for each different recipient using that particular recipient's public key. The encryption server has more computing resources available to it than an individual communication unit, and can encrypt and transmit a message multiple times to many different users in a more efficient manner than can an individual communication unit. Individual communication units need not store all possible recipient's public keys, but instead need store only the encryption server's public key. Encryption of the recipient's ID(s) helps to secure the identity of the recipient(s) and eliminates a source of information for traffic analysis by undesired readers/interceptors of such information.

What is claimed is:

1. A method comprising the steps of:

at a communication unit operated by a user:

generating a digital data message;

encrypting the digital data message using a first key, yielding a first encrypted message;

appending an identification of the user and an identification of a first recipient to the first encrypted message, yielding an appended first encrypted message;

encrypting the appended first encrypted message using a second key, yielding a second encrypted message;

transmitting the second encrypted message to an encryption server;

at the encryption server:

receiving the second encrypted message;

decrypting the second encrypted message using a third key, yielding the appended first encrypted message;

determining the first encrypted message, the identification of the user, and the identification of the first recipient from the appended first encrypted message;

encrypting the first encrypted message and the identification of the user with a fourth key, yielding a third encrypted message;

transmitting the third encrypted message to the first recipient.

2. The method of claim 1, wherein the step of appending further comprises the step of appending an identification of a second recipient to the first encrypted message, thereby yielding the appended first encrypted message.

3. The method of claim 2, further comprising the steps of encrypting, by the encryption server, the first encrypted message and the identification of the user with a fifth key, yielding a fourth encrypted message, and transmitting the fourth encrypted message to the second recipient.

4. The method of claim 3, wherein the fifth key is a public key associated with the second recipient.

5. The method of claim 1, wherein the first key is a private key associated with the user.

6. The method of claim 1, wherein the second key is a public key associated with the encryption server.

7. The method of claim 1, wherein the third key is a private key associated with the encryption server.

8. The method of claim 1, wherein the fourth key is a public key associated with the first recipient.

9. The method of claim 1, wherein the second key and the third key are identical.

10. The method of claim 1, wherein the step of appending further comprises the step of appending three or more identifications of recipients to the first encrypted message, thereby yielding the appended first encrypted message.

11. The method of claim 1, wherein the steps of transmitting are performed over radio frequency communication resources.

12. A method comprising the steps of:

at a communication unit operated by a user:

generating a digital data message;

encrypting the digital data message using a first key, yielding a first encrypted message;

appending an identification of the user and an identification of a first recipient to the first encrypted message, yielding an appended first encrypted message;

encrypting the appended first encrypted message using a second key, yielding a second encrypted message;

transmitting the second encrypted message to the encryption server, wherein the encryption server is not the first recipient.

13. The method of claim 12, wherein the first key is a private key associated with the user.

14. The method of claim 13, wherein the second key is a public key associated with the encryption server.

15. The method of claim 12, wherein the step of appending further comprises the step of appending an identification of a second recipient to the first encrypted message, thereby yielding the appended first encrypted message.

16. A method comprising the steps of:

at an encryption server:

receiving a first encrypted message;

decrypting the encrypted message using a first key, yielding a decrypted message comprising a second encrypted message, an identification of a sender of the first encrypted message, and an identification of a first recipient;

determining the second encrypted message, the identification of the sender, and the identification of the first recipient from the decrypted message;

encrypting the second encrypted message and the identification of the sender with a second key, yielding a third encrypted message;

transmitting the third encrypted message to the first recipient.

17. The method of claim 16, wherein the first key is a private key associated with the encryption server.

18. The method of claim 16, wherein the second key is a public key associated with the first recipient.

19. The method of claim 16, further comprising, when a second identification of a second recipient is part of the decrypted message, the steps of encrypting, by the encryption server, the second encrypted message and the identification of the sender with a third key, yielding a fourth encrypted message, and transmitting the fourth encrypted message to the second recipient.

20. The method of claim 19, wherein the third key is a public key associated with the second recipient.

21. A method comprising the steps of:

at a communication unit operated by a user:

generating a digital data message;

encrypting the digital data message using a private key associated with the user, yielding a first encrypted message;

appending an identification of the user, a first identification of a first recipient, and a second identification of a second recipient to the first encrypted message, yielding an appended first encrypted message;

encrypting the appended first encrypted message using a public key associated with an encryption server, yielding a second encrypted message;

transmitting the second encrypted message to the encryption server;

at an encryption server:

receiving the second encrypted message;

decrypting the second encrypted message using a private key associated with the encryption server, yielding the appended first encrypted message;

determining the first encrypted message, the identification of the user, the identification of the first recipient, and the second identification of the second recipient from the appended first encrypted message;

encrypting the first encrypted message and the identification of the user with a first public key associated with the first recipient, yielding a third encrypted message;

transmitting the third encrypted message to the first recipient;

encrypting the first encrypted message and the identification of the user with a second public key associated with the second recipient, yielding a fourth encrypted message;

transmitting the fourth encrypted message to the second recipient.

22. A method comprising the steps of:

at a communication unit operated by a user:

generating a digital data message;

encrypting the digital data message using a first key, yielding a first encrypted message;

encrypting the first encrypted message using a second key, yielding a second encrypted message;

appending an identification of the user and an identification of a first recipient to the second encrypted message, yielding an appended second encrypted message;

transmitting the appended second encrypted message to the encryption server;

at the encryption server:

receiving the appended second encrypted message;

determining the second encrypted message, the identification of the user, and the identification of the first recipient from the appended second encrypted message;

decrypting the second encrypted message using a third key, yielding the first encrypted message;

encrypting the first encrypted message with a fourth key, yielding a third encrypted message;

transmitting the third encrypted message to the first recipient.

23. The method of claim 22, wherein the step of appending further comprises the step of appending an identification of a second recipient to the second encrypted message, thereby yielding the appended second encrypted message.

24. The method of claim 23, further comprising the steps of encrypting, by the encryption server, the first encrypted message and the identification of the user with a fifth key, yielding a fourth encrypted message, and transmitting the fourth encrypted message to the second recipient.

25. The method of claim 24, wherein the fifth key is a public key associated with the second recipient.

26. The method of claim 24, wherein the identification of the user is appended to the fourth encrypted message before transmitting takes place at the encryption server.

27. The method of claim 22, wherein the first key is a private key associated with the user.

28. The method of claim 22, wherein the second key is a public key associated with the encryption server.

29. The method of claim 22, wherein the third key is a private key associated with the encryption server.

30. The method of claim 22, wherein the fourth key is a public key associated with the first recipient.

31. The method of claim 22, wherein the identification of the user is encrypted using the second key before the step of appending.

32. The method of claim 22, wherein the identification of the user is appended to the first encrypted message before encrypting takes place at the encryption server.

33. The method of claim 22, wherein the step of appending further comprises the step of appending three or more identifications of recipients to the second encrypted message, thereby yielding the appended first encrypted message.

34. The method of claim 22, wherein the steps of transmitting are performed over radio frequency communication resources.

* * * * *